PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) **Classification internationale des brevets** 7 : **G07F 7/10**

A1

(11) **Numéro de publication internationale:** **WO 00/07153**

(43) **Date de publication internationale:** 10 février 2000 (10.02.00)

(21) **Numéro de la demande internationale:** PCT/FR99/01826

(22) **Date de dépôt international:** 26 juillet 1999 (26.07.99)

(30) **Données relatives à la priorité:**
98/09575 27 juillet 1998 (27.07.98) FR

(71) **Déposant** *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(72) **Inventeurs; et**
(75) **Inventeurs/Déposants** *(US seulement)*: DREHER, Dominique [FR/FR]; 69, avenue des Oliviers, F–83740 La Cadière (FR). IMBERT, Patrick [FR/FR]; Parc des 7 Collines, 35, rue de la Saoupe, F–13011 Marseille (FR).

(74) **Mandataire:** NONNENMACHER, Bernard; Gemplus S.C.A., Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(81) **Etats désignés:** AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

(54) **Title:** METHOD FOR CONTROLLING THE EXECUTION OF A REQUEST FOR ACTION TRANSMITTED BY A SERVER TO A CHIP CARD VIA A TERMINAL

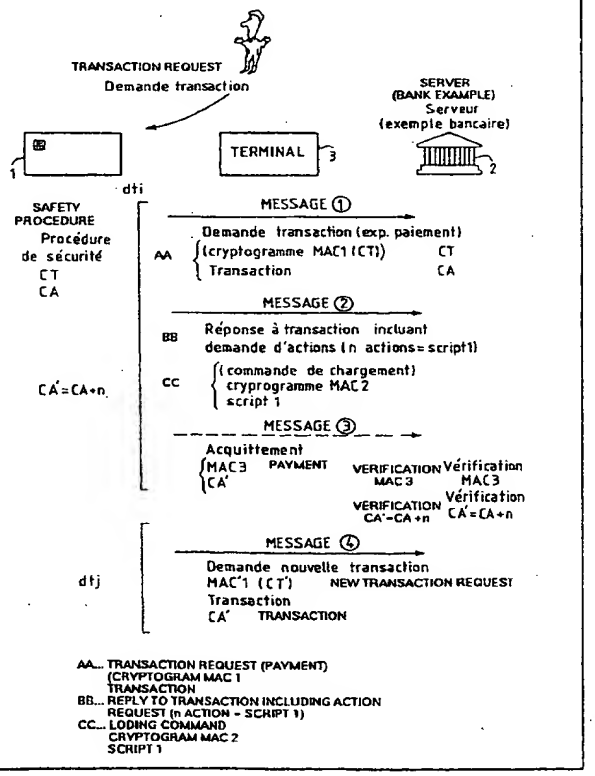
(54) **Titre:** PROCEDE DE CONTROLE DE L'EXECUTION D'UNE DEMANDE D'ACTIONS TRANSMISE PAR UN SERVEUR VERS UNE CARTE A PUCE VIA UN TERMINAL

(57) **Abstract**

The invention concerns a method for exchanging synchronised messages between an application server and at least a chip card, wherein the card transmits a message to the server containing the latest current value of an action counter stored by the server; the server emits a message comprising a request including one or several actions to be implemented by the card and stores the number n of actions of the request; the card receives the message, successively executes the action or actions in the request incrementing its action counter between each action if the action has been successfully executed; when there is a request for a transaction by the card, the server compares the received action counter value with the latest value stored, incremented by the number of actions contained in the previous request for actions and, operates on the basis of this comparison.

(57) **Abrégé**

L'invention concerne un procédé d'échange de messages avec synchronisation entre un serveur d'application et au moins une carte à puce. Pour cela la carte transmet un message au serveur contenant la dernière valeur courante d'un compteur d'actions que le serveur stocke; le serveur émet un message comportant une demande comprenant une ou plusieurs actions à mettre en oeuvre par la carte et stocke le nombre n d'actions de la demande; la carte reçoit le message, exécute successivement la ou les actions de la demande en incrémentant son compteur d'actions entre chaque action si l'action s'est bien exécutée; lors d'une demande de transaction par la carte, le serveur compare la valeur du compteur d'actions reçue, à la dernière valeur stockée, incrémentée du nombre d'actions contenues dans la demande d'actions précédente et, exploite le résultat de cette comparaison.



UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

PROCÉDÉ DE CONTROLE DE L'EXÉCUTION D'UNE DEMANDE D'ACTIONS TRANSMISE PAR UN SERVEUR VERS UNE CARTE A PUCE VIA UN TERMINAL

La présente invention concerne les systèmes d'échanges de messages entre serveur d'application et cartes à puce empruntant un réseau de communication. Elle s'applique aux échanges s'effectuant à travers les réseaux de télécommunication, réseau téléphonique commuté, réseau cellulaire ou réseau Internet.

Généralement, les messages échangés entre un serveur d'application et l'application correspondante dans une carte à puce transitent par un équipement intermédiaire que l'on désignera par terminal dans la suite. La carte à puce d'un utilisateur coopère avec le terminal pour permettre les échanges.

Dans le cas où le réseau emprunté est un réseau de téléphonie, le terminal est un terminal de télécommunication. Dans le cas où le réseau emprunté est un réseau informatique, le terminal est un équipement informatique de type ordinateur équipé d'une interface de lecture/écriture de cartes à puce.

Un serveur sous contrôle d'un organisme émetteur de carte, désirant effectuer une action sécurisée dans une carte à puce (ou dans une application de ladite carte) via un réseau téléphonique, utilise des certificats cryptographique permettant d'assurer la sécurité des échanges.

Cependant, en cas de perte d'un message durant la transmission ou l'exécution ou en cas de tentative de fraude, la re-synchronisation des messages serveur-cartes peut poser des problèmes sécuritaires.

Dans le cas où le terminal est un terminal dédié et sécurisé sous contrôle de l'organisme émetteur (par

exemple un distributeur automatique de billets DAB sous contrôle d'une banque), la perte d'un message est compensée par des mécanismes de synchronisation mettant en jeu à la fois le logiciel du serveur et le logiciel du terminal dédié. Le terminal dédié est sécurisé soit physiquement (DAB) soit contient à l'intérieur un module SAM (Secure Authentication Module), et dans tous les cas est contrôlé étroitement par l'organisme émetteur.

Si le terminal utilisé n'est pas un terminal dédié et sécurisé (par exemple téléphone GSM, PC sous Internet,...), les mécanismes de synchronisation ne peuvent pas être basés sur la sécurité du terminal, du fait que celui-ci n'est pas contrôlable par l'émetteur.

En effet, il est important de pouvoir re-synchroniser la source des messages et la carte à puce en cas de problème de transmission sur le réseau. Ce problème a été posé en terme de sécurité vis-à-vis des opérateurs et des fournisseurs de service.

Il n'existe pas à ce jour de système prévu pour assurer une synchronisation entre la carte et le serveur, dans les cas où pendant une transaction en cours, acceptée par conséquent par la carte, le serveur profite de la connexion pour envoyer un message comportant une ou plusieurs actions à mettre en oeuvre par la carte, ces actions pouvant être par exemple un rechargement d'unités de valeur ou de paramètres (monétaires ou autre) ou un chargement d'une nouvelle application.

En effet, il est prévu dans le cadre plus général des cartes multi-applicatives, que des message soient envoyés alors que l'utilisateur a fait une demande de transaction afin d'envoyer des commandes pour des

actions à entreprendre pendant le déroulement de l'application pour la transaction en cours.

De tels messages permettront par exemple de commander un rechargement de porte-monnaie électronique dans le cas d'une application porte-monnaie électronique, ou de modifier des paramètres bancaires de l'application bancaire, ou le chargement d'une nouvelle application dans la carte.

Il est clair que dans cette situation, le serveur ne sera pas informé dans le cas où ledit message est perdu.

En d'autres termes, effectuer des actions sécurisées sur un terminal non dédié est faisable aujourd'hui mais impose, soit des contraintes utilisateur fortes (cartes ou applications bloquées si l'action sécuritaire n'est pas parvenue à terme), soit des risques de perte d'informations (par exemple perte d'une transaction de rechargement d'un porte-monnaie électronique).

Le but de l'invention est que le serveur puisse détecter les défauts d'exécution d'une ou plusieurs actions ou commandes, liés à une perte de messages entre le serveur et la carte à puce ou à des défauts d'exécution d'actions dans la carte, lesdits messages ayant été transmis à la carte éventuellement pendant une transaction en cours, ceci afin d'en informer le serveur pour que ce dernier détermine quelles sont les dernières actions ou commandes non exécutées par la carte.

Selon une procédure pré-établie en fonction de la ou des actions non mises en oeuvre, le serveur pourra par exemple renvoyer le message contenant la dite ou les dites actions et permettre leur exécution.

A cette fin, l'invention a particulièrement pour objet un procédé de contrôle de l'exécution d'une demande d'actions transmise par un serveur vers une carte via un terminal, ladite carte comportant un compteur d'actions, caractérisé en ce qu'il comporte les étapes suivantes :

a) à l'émission par le serveur d'un message comportant une demande comprenant une ou plusieurs actions à mettre en oeuvre par la carte, le serveur stocke le nombre n d'action de la demande;

b) à la réception du message, la carte exécute successivement la ou les actions de la demande en incrémentant son compteur d'actions entre chaque actions si l'action s'est bien exécutée et en refusant cette action et les actions successives si l'action ne s'est pas bien exécutée sans incrémenter son compteur.

c) on compare la variation entre la valeur dans la carte et celle stockée dans le serveur et on détermine que les x dernières actions (commandes) ne sont pas exécutées si le résultat de la comparaison présente un écart de x.

L'incrémentation du compteur d'action correspond au nombre d'actions correctement exécutées.

Le nombre x est égal à 0 si toutes les actions sont correctement éxécutées, ce nombre x peut donc varier de 1 à n si la dernière ou toutes les actions ont échoué.

Pour comparer la variation entre la valeur dans la carte et celle stockée dans le serveur, la carte transmet au serveur la valeur courante de son compteur avant et après exécution de la commande d'actions.

Pour comparer la variation entre la valeur dans la carte et celle stockée dans le serveur, la carte calcule la valeur de la variation de son compteur suite

à l'exécution de la commande d'actions et la transmet au serveur.

Selon une autre caractéristique, tout échange de la valeur du compteur d'actions de la carte est effectué systématiquement de manière sécurisé.

A cette fin, la dernière valeur du compteur d'actions de la carte est transmise avec un cryptogramme dont le calcul implique la dite dernière valeur.

Selon une autre caractéristique la dernière valeur courante du compteur d'actions de la carte est transmise au serveur en temps réel, c'est-à-dire pendant la transaction en cours.

Selon un exemple la valeur pourra être transmise au moyen du message d'acquittement de la transaction en cours dans la carte.

Selon une autre caractéristique la valeur du compteur d'actions de la carte est transmise au serveur en temps différé.

Selon un exemple la valeur du compteur d'actions pourra être transmise au moyen d'un message d'une nouvelle demande de transaction par la carte par le serveur.

Selon un autre exemple la valeur du compteur d'actions de la carte est transmise au moyen d'un message d'information émis pour la carte au serveur.

L'invention a également pour objet une carte pour mettre en oeuvre le procédé précité comportant un compteur et des moyens de gestion de ce compteur, caractérisée en ce que lesdits moyens de gestion sont aptes à incrémenter ledit compteur d'actions entre chaque action si l'action s'est bien exécutées et à ne pas l'incrémenter pour cette action ni pour les actions suivantes si cette action n'a pas été exécutée.

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description ci-après donnée à titre d'exemple non limitatif et en regard des dessins sur lesquels :

- la figure 1, illustre des échanges de messages entre serveur et carte à puce selon l'invention,
- la figure 2, illustre de manière détaillée des échanges de messages entre serveur et carte à puce dans le cas d'une perte de message,
- la figure 3, illustre un autre cas de perte de message.

On entend par demande d'actions, un message comportant un jeu de n commandes, n pouvant bien entendu être égal à 1.

On pourra se reporter pour mieux comprendre la suite au schéma de la figure 1.

Dans toute la suite, on a pris comme exemple le cas où le serveur 2 profite d'une transaction en cours dans une carte 1 pour lui envoyer une demande comportant une ou plusieurs actions que la carte devra exécuter.

Bien entendu dans ce cas une demande d'action sera émise avec la réponse à la transaction en cours si ladite transaction nécessite une réponse. Si ce n'est pas le cas, crée une réponse contenant uniquement la demande d'actions. Le terminal qui est en communication avec le serveur reçoit le message correspondant à cette réponse, épure ce message de son enveloppe pour transmettre les actions à la carte.

Une demande d'actions peut comporter plusieurs actions à entreprendre par la carte, c'est-à-dire comme précisé au début de la description, un jeu de n commandes.

A titre d'exemple une demande d'actions pourra être une demande de changement d'un ou plusieurs paramètres dans un programme d'application ou, le chargement d'une nouvelle application ou, le chargement d'unités de valeur.

Le changement d'un paramètre correspond à une action pour la carte qui est une opération d'effacement et écriture à une adresse prédéterminée.

Le changement de plusieurs paramètres correspond à autant d'opérations d'effacement et écriture à des adresse distinctes que de paramètres et par conséquent à autant d'actions à entreprendre qu'il y a de paramètres à changer.

On va maintenant détailler ce qui se passe côté carte et côté serveur.

Côté carte :

La carte 1 incrémente après chaque action correctement effectuée, le compteur d'actions CA dès qu'elle reçoit du serveur une ou plusieurs actions à entreprendre et qu'elle a pu mener à bien l'exécution de chacune de ces actions.

La valeur du compteur est remontée vers le serveur par exemple chaque fois que la carte envoie un message au serveur (message 3 ou message 4 sur la figure 1).

La valeur du compteur peut être remontée vers le serveur 2 essentiellement lors des actions suivantes :

- lorsqu'il y a un acquittement de transaction (si durant une transaction un message d'acquittement est remonté au serveur on peut mettre dans cet acquittement la valeur du compteur d'actions), (exemple : message 3),
- lorsqu'il y a une demande de transaction ou d'authentification de la carte vers le serveur, (exemple : message 4),

- dans le cas de cartes bancaires ou de porte-monnaie électronique :

- on stocke dans chaque terminal 3 toute transaction passée,

- la transaction stockée est remontée au serveur pour que le serveur puisse enclencher le processus de paiement du marchand auprès duquel a eu lieu la transaction, le compteur d'actions CA peut être remonté avec cette transaction.

Ainsi, la valeur du contenu du compteur d'actions est toujours remontée au serveur soit en temps réel lorsque cela est fait lors d'un acquittement ou en temps différé lors d'une nouvelle demande de transaction ou lors d'une remontée d'un stockage de transactions.

Côté serveur :

Pour chaque carte contenant une application qui lui est dédiée ayant une demande d'actions en cours, le serveur doit stocker :

- le numéro d'identification de l'application,
- la valeur courante du compteur d'actions,
- la liste des actions en cours pour cette carte.

Ainsi, le serveur auquel appartient une application placée dans une carte à puce multi-applicative, peut lors de n'importe quelle transaction demandée par la carte, commander une action telle qu'un rechargement d'unités, ou qu'un chargement d'un programme ou qu'un chargement de nouveaux paramètres pour un programme résidant dans la carte.,

Le serveur peut ainsi envoyer des actions à la carte par un mécanisme de script non interprétable par le terminal 3, qui se trouve entre le serveur et la carte pour assurer la communication. Le terminal 3

transmet le ou les messages reçus dans le script à la carte de manière transparente.

On va maintenant détailler l'ensemble des traitements dans le cas où la remontée du contenu du compteur d'actions se fait en temps réel et dans le cas où tout se passe bien, c'est-à-dire dans le cas où il n'y a pas de perte de message et où l'exécution par la carte s'est bien déroulée.

On pourra se reporter au mode de réalisation particulier illustré par le schéma de la figure 1 pour mieux comprendre.

- A l'instant dti le porteur demande via son terminal 3 une transaction (un paiement ou une autre transaction) : message 1.

- La carte prépare la transaction et un cryptogramme, c'est-à-dire les données d'authentification, désignées par la suite par MAC et transmet au terminal.

Associé à cette transaction, l'application bancaire joint la valeur actuelle CA de son compteur d'actions sécurisé par le cryptogramme.

- Le terminal remonte la transaction au serveur bancaire.

De façon pratique, la carte envoie un message de demande de transaction contenant les données MAC1 ainsi que la valeur du compteur d'action CA, et l'identification de la transaction demandée.

- Le serveur vérifie les données d'authentification de la carte MAC1 et traite la transaction. Le serveur peut à ce moment effectuer une action dans l'application de la carte.

Selon un exemple particulier, il peut s'agir d'un chargement de paramètre monétaire dans la carte, mais

comme cela a été dit, d'autres actions du type rechargement d'un porte-monnaie électronique sont également possibles.

- Pour cela, le serveur va préparer une ou plusieurs commandes de chargement de paramètres contenues dans un champ d'information dénommé ci-après script 1, et les données d'authentification sécuritaire MAC2.

- La demande d'action est envoyée par un message 2 qui peut contenir la réponse à la transaction en cours si une telle réponse est prévue pour l'application concernée.

Au moment de l'envoi du script 1 à la carte, le serveur stocke dans une base de donnée ce script 1, en y associant les données relatives à la carte, ainsi que la valeur courante CA du compteur d'actions de la carte (remontée de la carte vers le serveur durant la demande de transaction). Ces informations vont permettre d'effectuer la synchronisation serveur-carte.

- La carte qui reçoit les commandes une à une du script 1, vérifie le cryptogramme MAC2, et effectue de manière atomique (c'est-à-dire en une fois et de manière indivisible) action par action de la liste du script 1 et incrémente le contenu CA du compteur après chaque action si celle-ci s'est bien déroulée. Lorsqu'une action s'est mal déroulée, le compteur d'action n'est pas incrémenté et les autres actions ne sont pas acceptées.

- Afin de remonter au serveur la nouvelle valeur CA' du compteur d'actions CA de la carte, plusieurs schémas sont possibles :

- remontée lors d'un message d'acquittement de la transaction en cours c'est-à-dire en temps réel, (correspond au message 3 de la transaction en cours);

- remontée de la valeur du CA' durant la prochaine transaction, (correspond au message 4 se produisant à l'instant dtj);

- à n'importe quel moment c'est à dire lorsque la carte envoie des informations au serveur.

- Dans le cas de l'exemple décrit, la carte renvoie un acquittement sécurisé au serveur incluant le contenu CA' en temps réel. Celui-ci peut alors comparer la valeur retournée par l'acquittement avec la valeur stockée dans sa base.

Si la valeur CA' = CA+n, n étant le nombres d'actions du script 1, ceci prouve que le script 1 s'est déroulé correctement dans la carte. Le serveur peut alors effacer ce script dans la base de données.

On va maintenant décrire en relation avec la figure 2, en reprenant le même exemple, ce qui se passe lorsque se produit une coupure ou une perte du message de demande d'actions (message 2).

Dans ce cas de figure, la commande script 1 n'est pas arrivée dans la carte. Le serveur va devoir se resynchroniser. Le serveur est informé de cette situation car selon cet exemple il n'a pas reçu d'acquittement.

Dans les cas où le serveur n'attend pas d'acquittement, il est informé lorsqu'il reçoit la dernière valeur du compteur d'action de la carte c'est à dire par exemple lors de la prochaine transaction.

En effet, durant l'authentification de la carte par le serveur (vérification MAC1), le serveur identifie que cette carte n'a pas reçu le script 1 (ou que le script 1 n'a pas été effectué correctement dans la carte) grâce à la valeur CA' du compteur d'actions qui

est remontée au serveur et comparée à la valeur CA stockée dans le serveur.

Si CA' est inférieur à CA et non égal, cela veut dire que la dernière ou les dernières actions n'ont pas été effectuées correctement.

Dans ce cas le serveur remet à jour sa base de données DB, en effaçant la valeur CA pour mettre la valeur CA'. Le serveur est à nouveau synchronisé et peut relancer la ou les dernières actions non exécutées par la carte.

On va maintenant décrire en relation avec la figure 3, en reprenant toujours le même exemple, ce qui se passe lorsque se produit une coupure lors du message d'acquittement.

Ce cas ne peut être envisagé que dans le cas où un message d'acquittement est prévu par l'application. Mais le même problème peut se produire lorsque la remontée du compteur d'actions est effectuée au moment d'une demande d'une nouvelle transaction, ou de l'envoi d'un message d'information.

Dans ce cas de figure, lors de la nouvelle demande de transaction, la valeur courante du compteur d'actions de la carte CA' = CA+n est remontée.

Le serveur compare cette valeur CA' à sa dernière valeur stockée, c'est-à-dire CA. Comme CA' = CA+n, le serveur sait que les n dernières actions ont bien été menées, il stocke la nouvelle valeur du compteur d'actions, c'est-à-dire CA+n pour être synchronisé avec la carte.

REVENDICATIONS

1. Procédé de contrôle de l'exécution d'une demande d'actions transmise par un serveur vers une carte via un terminal, ladite carte comportant un compteur d'actions, caractérisé en ce qu'il comporte les étapes suivantes :

a) à l'émission par le serveur d'un message comportant une demande comprenant une ou plusieurs actions à mettre en oeuvre par la carte, le serveur stocke le nombre n d'action de la demande;

b) à la réception du message, la carte exécute successivement la ou les actions de la demande en incrémentant son compteur d'actions entre chaque actions si l'action s'est bien exécutée et en refusant cette action et les actions successives si l'action ne s'est pas bien exécutée sans incrémenter son compteur.

c) on compare la variation entre la valeur dans la carte et celle stockée dans le serveur et on détermine que les x dernières actions (commandes) ne sont pas exécutées si le résultat de la comparaison présente un écart de x.

2. Procédé selon la revendication 1, caractérisé en ce que pour comparer la variation entre la valeur dans la carte et celle stockée dans le serveur, la carte transmet au serveur la valeur courante de son compteur avant et après exécution de la commande d'actions.

3. Procédé selon la revendication 1, caractérisée en ce que pour comparer la variation entre la valeur dans la carte et celle stockée dans le serveur, la carte calcule la valeur de la variation de son compteur

suite à l'exécution de la commande d'actions et la transmet au serveur.

4. Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que la carte transmet ledites valeurs sous forme sécurisée.

5. Procédé d'échange de messages selon la revendication 1, caractérisé en ce que la valeur du compteur d'actions de la carte est transmise en temps réel, c'est-à-dire pendant la transaction en cours.

6. Procédé d'échange de messages selon la revendication 5, caractérisé en ce que la valeur du compteur d'actions de la carte est transmise au serveur au moyen du message d'acquittement de la transaction en cours dans la carte.

7. Procédé d'échange de messages selon la revendication 1, caractérisé en ce que la valeur du compteur d'actions de la carte est transmise en temps différé.

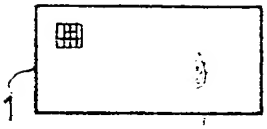
8. Procédé d'échange de messages selon la revendication 7, caractérisé en ce que la valeur du compteur d'actions de la carte est transmise au serveur au moyen d'un message d'une nouvelle demande de transaction par la carte pour le serveur.

9. Procédé d'échange de messages selon la revendication 7, caractérisé en ce que la valeur du compteur d'actions de la carte est transmise au moyen d'un message d'information émis par la carte au serveur.

10. Carte pour mettre en oeuvre le procédé selon l'une des revendications précédentes comportant un compteur et des moyens de gestion de ce compteur, caractérisée en ce que lesdits moyens de gestion sont aptes à incrémenter ledit compteur d'actions entre chaque action si l'action s'est bien exécutées et à ne pas l'incrémenter pour cette action ni pour les actions suivantes si cette action n'a pas été exécutée.

THIS PAGE BLANK (USPTO)

Demande transaction



TERMINAL 3

Serveur
(exemple bancaire)

dti

MESSAGE ①

Demande transaction (exp. paiement)
(cryptogramme MAC1 (CT)) CT
Transaction CA

Procédure
de sécurité
CT
CA

MESSAGE ②

Réponse à transaction incluant
demande d'actions (n actions = script1)
(commande de chargement)
cryprogramme MAC 2
script 1

CA' = CA+n

MESSAGE ③

Acquittement
MAC3
CA'

Vérification
MAC3
Vérification
CA' = CA+n

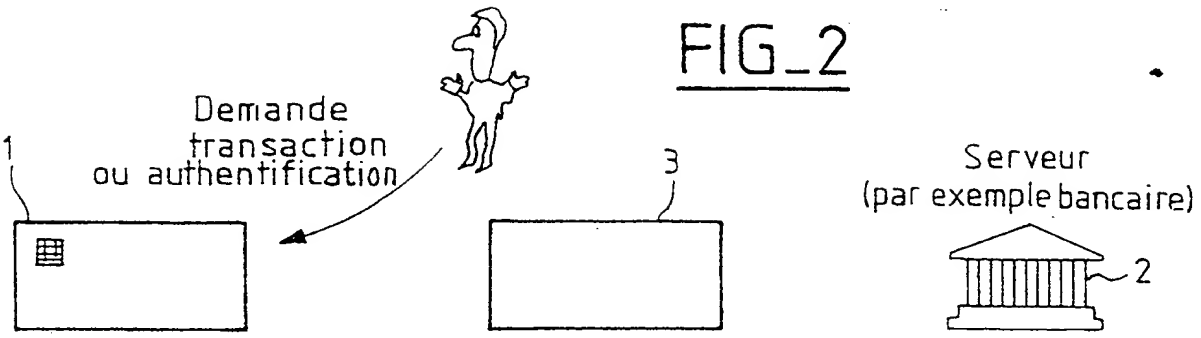
MESSAGE ④

Demande nouvelle transaction
MAC'1 (CT')
Transaction
CA'

dtj

FIG_1

FIG_2



Application
- Calcul données d'authentification carte MAC1
- Lecture compteur d'action CA

MESSAGE ①

Demande de transaction
- MAC1
- CA
- Transaction bancaire

- Vérification MAC1
- Effectue la transaction
- Calcul donnée d'authentification serveur MAC 2
- Préparation commande de changement de paramètre script1
- Stockage CA et script1 dans DB serveur

Exemple coupure de ligne

MESSAGE ②

Réponse à transaction incluant demande d'actions (script1)

{Commande de chargement MAC2, script1

MESSAGE ③

Application
- Calcul données d'authentification carte MAC1
- Lecture compteur d'action CA

Nouvelle demande de transaction
{- MAC1, CA
{- Transaction bancaire

- Vérification MAC1
- Vérification $CA_{carte} = CA_{serveur} \Rightarrow$ annule la dernière transaction
- Calcul MAC2
- Préparation nouveau script 2

Stockage CA' et script 2 dans DB serveur

MESSAGE ④

Réponse à transaction incluant demande d actions (script 2)

{Commande de chargement MAC 2, Script 2

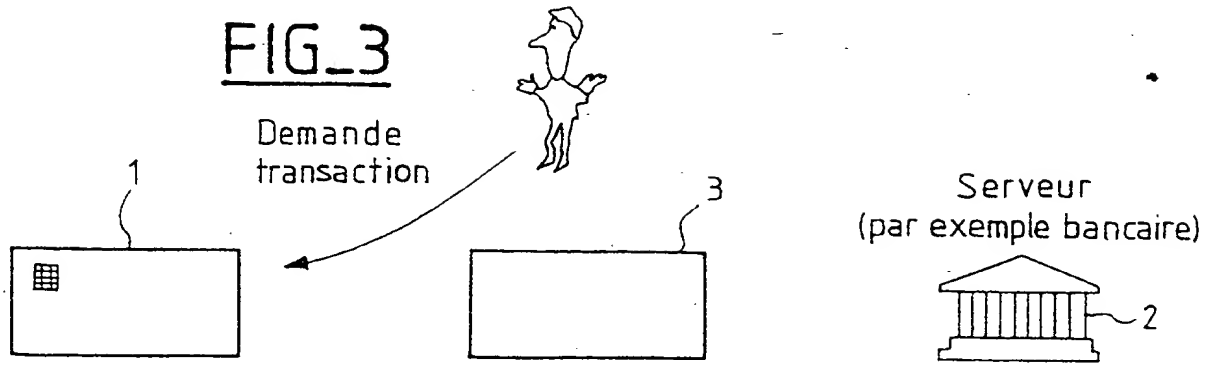
- Vérification MAC2
- Si MAC2 ok alors effectue script 2
- Si script1 ok, incrémentation CA = CA +1
- Calcul MAC3 d'acquittement

MESSAGE ⑤

Acquittement MAC3, CA+1

- Vérification MAC3
- Vérification CA' = CA+1
- Effacement DB

FIG_3



Application
- Calcul données d'authentification carte MAC1
- Lecteur compteur d'action CA

MESSAGE ①

Demande de transaction
- MAC1
- CA
- Transaction bancaire

- Vérification MAC1
- Effectue la transaction
- Calcul donnée d'authentification serveur MAC 2
- Préparation commande de changement de paramètre script1
- Stockage CA et script dans DB serveur

MESSAGE ②

Réponse à transaction incluant demande d'action (script1)
{Commande de chargement MAC2, Script1

- Vérification MAC2
- si MAC2 ok alors effectue script1
- si script1 ok incrémentation CA'=CA+1
- Calcul MAC3 d'acquittement

MESSAGE ③ (exemple coupure de ligne)

Acquittement

MESSAGE ④

Application
- Calcul données d'authentification carte MAC1
- Lecture compteur d'action CA'=CA+n

Nouvelle demande d'action
- MAC1, CA'
- Transaction bancaire

- Vérification MAC1
- Vérification CA'carte = CA+n dernière transaction OK
- Effectue la transaction courante
- Calcul MAC2
- Préparation nouveau script 2
- Stockage CA' et script 2 dans DB serveur

MESSAGE ⑤

Réponse à transaction incluant demande d'action (script 2)
{Commande de chargement MAC2, Script2

- Vérification MAC2
- si MAC2 ok alors effectue script2
- si script 1 ok, incrémentation CA'= CA'+1
- Calcul MAC3 d'acquittement

MESSAGE ⑥

Acquittement MAC3, CA"

- Vérification MAC3
- Vérification CA"=CA'+1
- Effacement DB

INTERNATIONAL SEARCH REPORT

onal Application No
PCT/FR 99/01826

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 0 795 844 A (NEDERLAND PTT) 17 September 1997 (1997-09-17) column 3, line 31 -column 6, line 54; figure 5	1,10 2-9
X	FR 2 748 880 A (GEMPLUS CARD INT) 21 November 1997 (1997-11-21) page 5, line 8 -page 8, line 17; claims 1,2,4-7,12-17; figures 1-6 page 11, line 4 -page 13, line 10 page 20, line 15 -page 22, line 19	10
E	FR 2 775 375 A (SOLAIC SA) 27 August 1999 (1999-08-27) the whole document	1,10

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 December 1999	22/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Guivol, O

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 716 021 A (GEMPLUS CARD INT) 11 August 1995 (1995-08-11) page 4, line 25 -page 7, line 5; claims 1,3-6; figures 2,3 page 8, line 33 -page 14, line 24; claims 1-4	1,10
A	US 5 161 231 A (IIJIMA YASUO) 3 November 1992 (1992-11-03) abstract; claims 1-6; figures 8-15	1,2,10
A	FR 2 757 664 A (BULL CP8) 26 June 1998 (1998-06-26) abstract; claims	1,10
A	US 4 654 480 A (WEISS JEFFREY A) 31 March 1987 (1987-03-31) the whole document	10
A	EP 0 789 336 A (DEUTSCHE TELEKOM AG) 13 August 1997 (1997-08-13) the whole document	10

INTERNATIONAL SEARCH REPORT

information on patent family members

onal Application No
PCT/FR 99/01826

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0795844 A	17-09-1997	AU 711427 B	14-10-1999
		AU 2154097 A	01-10-1997
		CA 2245944 A	18-09-1997
		WO 9734266 A	18-09-1997
		EP 0960403 A	01-12-1999
		JP 11506240 T	02-06-1999
		NZ 331257 A	28-10-1999
		US 5856659 A	05-01-1999
FR 2748880 A	21-11-1997	FR 2748834 A	21-11-1997
		AU 3697997 A	09-02-1998
		CA 2259287 A	22-01-1998
		CN 1230324 A	29-09-1999
		EP 0910923 A	28-04-1999
		WO 9803026 A	22-01-1998
		AU 3035797 A	09-12-1997
		CA 2255593 A	27-11-1997
		EP 0906603 A	07-04-1999
		WO 9744762 A	27-11-1997
FR 2775375 A	27-08-1999	WO 9942960 A	26-08-1999
FR 2716021 A	11-08-1995	AT 156922 T	15-08-1997
		DE 69500561 D	18-09-1997
		DE 69500561 T	11-12-1997
		EP 0744063 A	27-11-1996
		ES 2105892 T	16-10-1997
		WO 9522125 A	17-08-1995
		US 5731576 A	24-03-1998
US 5161231 A	03-11-1992	JP 63083892 A	14-04-1988
		JP 63126084 A	30-05-1988
		DE 3731736 A	07-04-1988
		FR 2604541 A	01-04-1988
		FR 2622318 A	28-04-1989
		FR 2684466 A	04-06-1993
FR 2757664 A	26-06-1998	AU 5668298 A	17-07-1998
		CA 2247474 A	02-07-1998
		CN 1212065 A	24-03-1999
		EP 0907937 A	14-04-1999
		WO 9828720 A	02-07-1998
		JP 11504748 T	27-04-1999
		NO 983851 A	21-10-1998
US 4654480 A	31-03-1987	AU 6470186 A	01-07-1987
		CA 1268258 A	24-04-1990
		EP 0248028 A	09-12-1987
		JP 63502393 T	08-09-1988
		US 4754482 A	28-06-1988
		WO 8703442 A	04-06-1987
EP 0789336 A	13-08-1997	DE 19604876 C	04-09-1997

RAPPORT DE RECHERCHE INTERNATIONALE

le internationale No
PCT/FR 99/01826

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10

Selon la classification internationale des brevets (CIB) ou a la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultee (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relevent des domaines sur lesquels a porte la recherche

Base de donnees électronique consultee au cours de la recherche internationale (nom de la base de donnees, et si realisable, termes de recherche utilises)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas echéant, l'indication des passages pertinents	no. des revendications visees
X A	EP 0 795 844 A (NEDERLAND PTT) 17 septembre 1997 (1997-09-17) colonne 3, ligne 31 -colonne 6, ligne 54; figure 5	1,10 2-9
X	FR 2 748 880 A (GEMPLUS CARD INT) 21 novembre 1997 (1997-11-21) page 5, ligne 8 -page 8, ligne 17; revendications 1,2,4-7,12-17; figures 1-6 page 11, ligne 4 -page 13, ligne 10 page 20, ligne 15 -page 22, ligne 19	10
E	FR 2 775 375 A (SOLAIC SA) 27 août 1999 (1999-08-27) le document en entier	1,10

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiques en annexe

° Categories speciales de documents cités:

"A" document definissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison speciale (telle qu'indiquee)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais posterieurement à la date de priorite revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquee ne peut être consideree comme nouvelle ou comme impliquant une activite inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison etant evidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevee	Date d'expedition du present rapport de recherche internationale
15 décembre 1999	22/12/1999

Nom et adresse postale de l'administration chargee de la recherche internationale	Fonctionnaire autorisé
Office Europeen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl Fax: (+31–70) 340–3016	Guivol, O

Formulaire PCT/ISA/210 (deuxieme feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

e internationale No
PCT/FR 99/01826

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	FR 2 716 021 A (GEMPLUS CARD INT) 11 août 1995 (1995-08-11) page 4, ligne 25 -page 7, ligne 5; revendications 1,3-6; figures 2,3 page 8, ligne 33 -page 14, ligne 24; revendications 1-4	1,10
A	US 5 161 231 A (IIJIMA YASUO) 3 novembre 1992 (1992-11-03) abrégé; revendications 1-6; figures 8-15	1,2,10
A	FR 2 757 664 A (BULL CP8) 26 juin 1998 (1998-06-26) abrégé; revendications	1,10
A	US 4 654 480 A (WEISS JEFFREY A) 31 mars 1987 (1987-03-31) le document en entier	10
A	EP 0 789 336 A (DEUTSCHE TELEKOM AG) 13 août 1997 (1997-08-13) le document en entier	10

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 99/01826

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)			Date de publication
EP 0795844	A	17-09-1997	AU	711427	B	14-10-1999
			AU	2154097	A	01-10-1997
			CA	2245944	A	18-09-1997
			WO	9734266	A	18-09-1997
			EP	0960403	A	01-12-1999
			JP	11506240	T	02-06-1999
			NZ	331257	A	28-10-1999
			US	5856659	A	05-01-1999
FR 2748880	A	21-11-1997	FR	2748834	A	21-11-1997
			AU	3697997	A	09-02-1998
			CA	2259287	A	22-01-1998
			CN	1230324	A	29-09-1999
			EP	0910923	A	28-04-1999
			WO	9803026	A	22-01-1998
			AU	3035797	A	09-12-1997
			CA	2255593	A	27-11-1997
			EP	0906603	A	07-04-1999
			WO	9744762	A	27-11-1997
FR 2775375	A	27-08-1999	WO	9942960	A	26-08-1999
FR 2716021	A	11-08-1995	AT	156922	T	15-08-1997
			DE	69500561	D	18-09-1997
			DE	69500561	T	11-12-1997
			EP	0744063	A	27-11-1996
			ES	2105892	T	16-10-1997
			WO	9522125	A	17-08-1995
			US	5731576	A	24-03-1998
US 5161231	A	03-11-1992	JP	63083892	A	14-04-1988
			JP	63126084	A	30-05-1988
			DE	3731736	A	07-04-1988
			FR	2604541	A	01-04-1988
			FR	2622318	A	28-04-1989
			FR	2684466	A	04-06-1993
FR 2757664	A	26-06-1998	AU	5668298	A	17-07-1998
			CA	2247474	A	02-07-1998
			CN	1212065	A	24-03-1999
			EP	0907937	A	14-04-1999
			WO	9828720	A	02-07-1998
			JP	11504748	T	27-04-1999
			NO	983851	A	21-10-1998
US 4654480	A	31-03-1987	AU	6470186	A	01-07-1987
			CA	1268258	A	24-04-1990
			EP	0248028	A	09-12-1987
			JP	63502393	T	08-09-1988
			US	4754482	A	28-06-1988
			WO	8703442	A	04-06-1987
EP 0789336	A	13-08-1997	DE	19604876	C	04-09-1997